

PATENT APPLICATION TRANSMITTAL LETTER
(Large Entity)

Docket No.
112857-221

TO THE ASSISTANT COMMISSIONER FOR PATENTS

#5

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

Tomoyuki Nakano et al.

For: AUTHENTICATION SYSTEM, AUTHENTICATION METHOD, AUTHENTICATION APPARATUS AND
AUTHENTICATION METHOD THEREFOR

Enclosed are:

- ☒ Certificate of Mailing with Express Mail Mailing Label No. EL416274860US
- ☒ thirteen sheets of drawings.
- ☒ A certified copy of a Japan application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☒ Other: Postcard

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	20	- 20 =	0	x \$18.00	\$0.00
Indep. Claims	4	- 3 =	1	x \$80.00	\$80.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$710.00
TOTAL FILING FEE					\$790.00

- ☒ A check in the amount of \$790.00 to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. 02-1818 as described below. A duplicate copy of this sheet is enclosed.
 - ☐ Charge the amount of as filing fee.
 - ☒ Credit any overpayment.
 - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
 - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: April 30, 2001


Signature

William E. Vaughan (Reg. No. 39,056)
Bell, Boyd & Lloyd LLC
P.O. Box 1135
Chicago, Illinois 60690

cc:

S 0649US00 #5

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC979 U.S. PTO
09/846522



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 4月28日

出 願 番 号

Application Number:

特願2000-131872

出 願 人

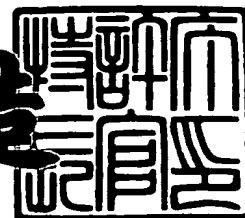
Applicant (s):

ソニー株式会社

2001年 3月 9日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3017751

【書類名】 特許願

【整理番号】 0000439304

【提出日】 平成12年 4月28日

【あて先】 特許庁長官 近藤 隆彦 殿

【国際特許分類】 H04L 9/00

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号ソニー株式会社内

 【氏名】 中野 智行

【発明者】

 【住所又は居所】 東京都品川区北品川6丁目7番35号ソニー株式会社内

 【氏名】 板橋 達夫

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082740

 【弁理士】

 【氏名又は名称】 田辺 恵基

【手数料の表示】

 【予納台帳番号】 048253

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9709125

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証システム、認証方法、認証装置及びその方法

【特許請求の範囲】

【請求項 1】

利用者に固有の共通鍵暗号方式による共通鍵を保持する情報保持媒体と、
各上記利用者ごとの上記共通鍵暗号方式による共通鍵と、公開鍵暗号方式による秘密鍵及び公開鍵とを保持する認証装置と、

上記認証装置と通信自在に接続され、公開鍵暗号方式による上記利用者の認証を行うための機能が実装された情報処理装置と

を具え、

上記認証装置は、

上記情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の上記情報保持媒体に保持された上記共通鍵と、自己が保持する当該利用者の上記共通鍵とに基づいて当該利用者の認証を行い、上記利用者を認証できた場合にのみ、当該利用者に対応する上記公開鍵及び上記秘密鍵を用いて、上記情報処理装置に当該利用者の認証を上記公開鍵暗号方式で行わせるための所定の処理を行う

ことを特徴とする認証システム。

【請求項 2】

上記情報保持媒体は、可搬型である

ことを特徴とする請求項 1 に記載の認証システム。

【請求項 3】

利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させる第 1 のステップと、

情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の上記情報保持媒体に保持された上記共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行う第 2 のステップと、

上記利用者を認証できた場合にのみ、上記情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う第 3 のステップと

を具えることを特徴する認証方法。

【請求項 4】

上記情報保持媒体は、可搬型である

ことを特徴とする請求項 3 に記載の認証方法。

【請求項 5】

各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する保持手段と、

外部の情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の上記共通暗号方式による上記共通鍵と、上記保持手段に保持された当該利用者の上記共通鍵とに基づいて当該利用者の認証を行い、上記利用者を認証できた場合にのみ、上記保持手段に保持された当該利用者に対応する上記公開鍵及び上記秘密鍵を用いて、上記情報処理装置に当該利用者の認証を上記公開鍵暗号方式で行わせるための所定の処理を行う処理手段と

を具えることを特徴とする認証装置。

【請求項 6】

各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する第 1 のステップと、

外部の情報処理装置から与えられる上記利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の上記共通暗号方式による上記共通鍵と、上記保持手段に保持された当該利用者の上記共通鍵とに基づいて当該利用者の認証を行い、上記利用者を認証できた場合にのみ、上記保持手段に保持された当該利用者に対応する上記公開鍵及び上記秘密鍵を用いて、上記情報処理装置に当該利用者の認証を上記公開鍵暗号方式で行わせるための所定の処理を行う第 2 のステップと

を具えることを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は認証システム、認証方法、認証装置及びその方法に関し、異なる種類の暗号方式の利点を効率良く利用し暗号処理し得る認証装置に適用して好適なものである。

【0002】

【従来の技術】

従来、この種の認証システムの認証及び署名方式として共通鍵暗号方式と公開鍵暗号方式がある。

【0003】

共通鍵暗号方式は、共通鍵と呼ばれる1つの暗号鍵を用い、共通鍵で暗号化した情報を同一の共通鍵で復号化する暗号方式である。共通鍵暗号方式は、暗号処理及び復号処理を短時間で行うことができるため、例えばICカードに格納された電子マネーや定期券情報という高速処理が要求される情報を処理する場合に利用される。

【0004】

また公開鍵暗号方式は、公開鍵及び暗号鍵と呼ばれる2つの暗号鍵を用いて、一方の暗号鍵で情報を暗号化したり、暗号化された情報を他方の暗号鍵で復号化する暗号方式である。公開鍵暗号方式は、かかる共通鍵暗号方式と比較して処理速度が遅いものの情報の漏洩に対する安全性が高く、インターネット等のネットワーク上で決済を行うときなどの匿名性が必要な場合に利用される。

【0005】

そして公開鍵暗号方式を用いる場合、ICカードには当該ICカードを使用する本人を証明する証明書と暗号鍵とが格納され、暗号処理を行うためのモジュールとして利用される。

【0006】

【発明が解決しようとする課題】

ところで認証システムにおいては、適用分野に応じてこれら共通鍵暗号方式及び公開鍵暗号方式を使い分けている。

【0007】

しかしながら近年では、一枚のICカードで効率良く認証や決済を行い得るよ

うにするために、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせ持つ暗号方式の統合が望まれている。

【0008】

また認証システムにおいては、ICカードに格納された証明書の正当性を検証する手段はあるが、当該ICカードが実際、正当に使用されているか否かを検証する手段がないという問題があった。

【0009】

さらに認証システムにおいては、ICカードが紛失された場合、ネットワーク上に設けられた認証局から定期的に配付される証明書の失効リストに基づいてICカードに対する認証や決済等の手続きを停止するため、ネットワーク上のすべてのポイントで即時かかるICカードの使用が停止されないという問題があった。

【0010】

本発明は以上の点を考慮してなされたもので、認証に対する安全性及び高速性を向上させ得る認証システム、認証方法、認証装置及びその方法を提案しようとするものである。

【0011】

【課題を解決するための手段】

かかる課題を解決するために本発明においては、認証システムにおいて、利用者に固有の共通鍵暗号方式による共通鍵を保持する情報保持媒体と、各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による秘密鍵及び公開鍵とを保持する認証装置と、認証装置と通信自在に接続され、公開鍵暗号方式による利用者の認証を行うための機能が実装された情報処理装置とを設け、認証装置が、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵と、自己が保持する当該利用者の共通鍵とに基づいて当該利用者の認証を行い、利用者を認証できた場合にのみ、当該利用者に対応する公開鍵及び秘密鍵を用いて、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うようにした。この結果この認証システムによれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせ

もたせた利用者認証を行うことができる。

【 0 0 1 2 】

また本発明においては、認証方法において、利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させる第1のステップと、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行う第2のステップと、利用者を認証できた場合にのみ、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う第3のステップとを設けるようにした。この結果この認証方法によれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができる。

【 0 0 1 3 】

さらに本発明においては、認証装置において、各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する保持手段と、外部の情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の共通暗号方式による共通鍵と、保持手段に保持された当該利用者の共通鍵とに基づいて当該利用者の認証を行い、利用者を認証できた場合にのみ、保持手段に保持された当該利用者に対応する公開鍵及び秘密鍵を用いて、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う処理手段とを設けるようにした。この結果この認証装置によれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができる。

【 0 0 1 4 】

さらに本発明においては、認証方法において、各利用者ごとの共通鍵暗号方式による共通鍵と、公開鍵暗号方式による公開鍵及び秘密鍵とを保持する第1のステップと、外部の情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された当該利用者の共通暗号方式による共通鍵と、保持手段に保持された当該利用者の共通鍵とに基づいて当該利用者の認証を行い、利用者を認証できた場合にのみ、保持手段に保持された当該利用者に対応する公開鍵及び秘密鍵を用いて、情報処理装置に当該利用者の認証を公開鍵暗号方式

で行わせるための所定の処理を行う第2のステップとを設けるようにした。この結果この認証装置によれば、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができる。

【0015】

【発明の実施の形態】

以下図面について、本発明の一実施形態に形態を詳述する。

【0016】

(1) 本実施の形態によるネットワークシステムの構成

図1において、1は全体として本実施の形態によるネットワークシステムを示し、サービスプロバイダ2に設置されたWWW(World Wide Web)サーバ3と、利用者端末4と、認証センタ5に設置されたセキュリティサーバ6とがインターネット7を介して接続されることにより構成されている。

【0017】

利用者端末4は、図2に示すように、CPU (Central Processing Unit) 10と、後述のような各種処理を実行するためのプログラムが格納されたROM (Read Only Memory) 11と、CPU 10のワークメモリとしてのRAM (Random Access Memory) 12と、入出力インターフェイスとしての入出力部14とがバス13を介して接続され、また当該入出力部14にモデム等からなるネットワークインターフェイス15と、ICカード読書き装置9と、キーボード、モニタ及びマウス等からなるコンソール17と、ハードディスク装置等からなる記憶装置18とが接続されて構成された一般的なパーソナルコンピュータである。

【0018】

また記憶装置18には、WWWブラウザプログラム19と、共通鍵暗号方式や公開鍵暗号方式に応じた暗号処理を管理するプログラムからなる暗号処理ライブラリ25と、かかるICカード読書き装置9用のICカードドライバ21とが記憶されている。

【0019】

そしてCPU 10は、記憶装置18に記憶されたWWWブラウザプログラム19をRAM 12上で展開して実行することにより、WWWブラウザ22 (図1)

として機能し、ネットワークインターフェイス 1 5 を介してインターネット 7 上で情報の送受信を行い得るようになされている。

【 0 0 2 0 】

また CPU 1 0 は、記憶装置 1 8 に記憶された暗号処理ライブラリ 2 0 のプログラムを RAM 1 2 上で展開して実行することにより、暗号処理モジュール 2 3 (図 1) として機能し、暗号処理を管理する。

【 0 0 2 1 】

また WWW ブラウザ 2 2 と暗号処理モジュール 2 3 との間には、例えば RSA 社が提供する PKCS #11(Public Key Cryptography Standard #11) 2 4 規格の API (Application Program Interface) が設けられており、WWW ブラウザ 2 2 と暗号処理モジュール 2 3 との間で情報の交換を容易にしている。

【 0 0 2 2 】

さらに CPU 1 0 は、記憶装置 1 8 に記憶された IC カードドライバ 2 1 を RAM 1 2 上で展開して実行することにより、IC カード読書き装置 9 を操作することができる。

【 0 0 2 3 】

この IC カード読書き装置 9 は、例えばブルートゥース(Bluetooth) 規格の無線機能を有しており、IC カード 8 から無線を介して読み出した情報を記憶装置 2 3 に送出すると共に、記憶装置 2 3 から送出された情報を無線を介して IC カード 8 に書き込み得るようになされている。

【 0 0 2 4 】

實際上 IC カード 8 は、図 3 に示すように、バス 2 6 に CPU 2 7 と、ROM 2 8 と、RAM 2 9 と、かかる IC カード読書き装置 9 と無線通信し得る無線通信インターフェイス 3 0 と、当該 IC カード 8 に割り当てられた利用者 ID 等の各種情報を格納した EEPROM(Electrically Erasable Programmable ROM) 3 1 とが接続され構成されている。

【 0 0 2 5 】

EEPROM 3 1 には、利用者 ID 用エリア 3 2 と、電子有価情報用エリア 3 3 と、共通鍵用エリア 3 4 とが設けられており、各エリアに利用者 ID と、電子

有価情報と、利用者ID用エリア36及び電子有価情報用エリア37に対して外部からのアクセスを許可するための共通鍵とがそれぞれ書き込まれる。

【0026】

そしてCPU27は、ROM28に格納された暗号処理用プログラムをRAM29上で展開して実行することにより、無線インターフェース30を介して得た共通鍵によって暗号化された情報（以下、これを共通鍵暗号化情報と呼ぶ）を、EEPROM31から読み出した共通鍵で復号化する。

【0027】

またCPU27は、共通鍵暗号化情報がEEPROM31から読み出した共通鍵で復号が正しく行われると、当該EEPROM31の各エリアへのアクセスを許可し、例えばEEPROM31の電子有価情報用エリア33に無線インターフェース30を介して得た電子有価情報を書き込むようになされている。

【0028】

一方サービスプロバイダ2に設けられたWWWサーバ3は、図4に示すように、CPU36と、ROM37と、RAM38とがバス39を介して入出力部40に接続されていると共に、当該入出力部40にインターネット7と接続するためのルータ等からなるネットワークインターフェース41と、キーボード、モニタ及びマウス等からなる管理用コンソール42と、記憶装置43とが接続されて構成されている。また記憶装置43には、WWWサーバプログラム44と、電子有価情報等のサービス用コンテンツ45とが格納されている。

【0029】

そしてCPU36は、記憶装置43に格納されたWWWサーバプログラム44をRAM38上で展開して実行することにより、WWWサーバ3（図1）として動作し、サービス用コンテンツ45をネットワークインターフェース41を介して提供し得るようになされている。

【0030】

これに対して認証センタ5に設けられたセキュリティサーバ6は、図5に示すように、CPU46と、ROM47と、RAM48とがバス49を介して入出力部50に接続されていると共に、当該入出力部50にインターネット7と接続す

るためのルータ等からなるネットワークインターフェイス 5 1 と、キーボード、モニタ及びマウス等からなる管理用コンソール 5 2 と、記憶装置 5 3 とが接続されて構成されている。また記憶装置 5 3 には、セキュリティサーバプログラム 5 4、後述する利用者証明データベース 5 5 及び共通鍵データベース 5 6 が格納されている。

【 0 0 3 1 】

そしてかかるセキュリティサーバ 6 の CPU 4 6 は、記憶装置 5 3 に格納されたセキュリティサーバプログラム 5 4 を RAM 4 8 上で展開して実行することにより、セキュリティサーバ 6 として動作する。

【 0 0 3 2 】

(2) 認証処理手順

ここでこのネットワークシステム 1 は、図 6 に示すように、利用者端末 4 が図 7 に示す自己を認証する認証処理手順 R T 1 に従って認証を行うと共に、セキュリティサーバ 6 が図 8 に示す認証処理手順 R T 2 に従って当該利用者端末 4 の認証を行うことにより、利用者端末 4 が電子有価情報を提供する WWW サーバ 3 に対して自己の正当性を証明することができる。

【 0 0 3 3 】

この場合まず利用者端末 4 は、WWW ブラウザ 2 2 を操作して、WWW サーバ 3 に対し当該利用者端末 4 に電子有価情報を要求する。

【 0 0 3 4 】

このとき WWW サーバ 3 は、まずランダムな文字列からなる試用文字を生成した後、当該生成した試用文字と共に、要求元の正当性を確認するために利用者端末 4 が認証されるための認証要求コマンド C 1 を当該利用者端末 4 に送出する。

【 0 0 3 5 】

そして利用者端末 4 の CPU 1 0 は、認証要求コマンド C 1 を受けとると、認証処理手順 R T 1 を開始し（ステップ S P 1）、受けとった当該認証要求コマンド C 1 及び試用文字を暗号処理モジュール 2 3 に送出する（ステップ S P 2）。

【 0 0 3 6 】

続けて CPU 1 0 は、IC カード読書き装置 9 を介して IC カード 8 から使用

者IDを読み出し、当該読み出した使用者IDと共に暗号処理モジュール23で受けとった認証要求コマンドC1及び試用文字をセキュリティサーバ6へ送出する（ステップSP3）。

【0037】

セキュリティサーバ6のCPU46は、認証要求コマンドC1を受けとると、認証処理手順RT2を開始し（ステップSP21）、受けとった使用者IDに対応する共通鍵を、図9に示すような記憶装置53内の共通鍵データベース56から読み出し（ステップSP22）、当該読み出した共通鍵で共通暗号化情報を生成する。続けてCPU46は、共通暗号化情報と共にICカード認証要求コマンドC2を利用者端末4の暗号処理モジュール23に送出する（ステップSP23）。

【0038】

さらにCPU46は、かかる使用者IDに対応する証明書を、図10に示すような記憶装置53内の利用者証明データベース55から読み出し、これを利用者端末4の暗号処理モジュール23及びWWWブラウザ22を介してWWWサーバ4へ予め送出しておく。

【0039】

ここで証明書58には、例えば利用者IDが0001の場合、図11に示すように、証明書シリアル番号と、当該証明書の有効期限情報と、利用者IDと、かかる秘密鍵と対で生成された公開鍵と、電子メールのメールアドレスと、利用者の連絡先情報となどの情報が記載されている。加えて証明書58には、秘密鍵及び公開鍵（以下、これらの一組の鍵を暗号鍵と呼ぶ）を生成する認証局のデジタル署名60が施されており、当該証明書58の正当性を保証している。

【0040】

一方利用者端末4のCPU10は、暗号処理モジュール11においてICカード認証要求コマンド及び共通鍵を受けとると、ICカードドライバ21を実行することによりICカード読書き装置9を操作し（ステップSP5）、当該ICカード読書き装置9を介してICカード8にICカード認証要求コマンドC2及び共通暗号化情報を送出する。

【0041】

またICカード8は、ICカード認証要求コマンドC2を受けとると、共通暗号化情報を内部に設けられたEEPROM31内の共通鍵で認証（復号）し、当該認証結果を暗号処理モジュール23を介してセキュリティサーバ6に送出する（ステップSP5）。

【0042】

セキュリティサーバ6のCPU46は、受けとった認証結果によりICカード8の認証が正常に行われたことを確認すると（ステップSP15）、WWWサーバ3から送信された認証要求に基づいて、利用者証明データベース55（図6）から利用者IDの秘密鍵を取得し（ステップSP16）、受けとった試用文字に当該秘密鍵でデジタル署名を施してデジタル署名書（ステップSP17）を生成し、これを利用端末4の暗号処理モジュール23（ステップSP18）に送出する。

【0043】

これとは反対にCPU46は、受けとった認証結果によりICカード8の認証が正常に行えなかったことを確認すると（ステップSP15）、再度利用者IDを受けとり、当該利用者IDに応じた共通鍵で新しい共通暗号化情報を生成し、これをICカード8へ送出する。CPU46は、ICカード8から再度認証結果を得るようになされている。

【0044】

一方利用端末4のCPU10は、暗号処理モジュール23において、セキュリティサーバ6からデジタル署名書を受けとる（ステップSP7）と、これをPKCS#1124を介してWWWブラウザ10へ送出する（ステップSP8）。続けてCPU10は、受けとったデジタル署名書を認証要求の応答としてWWWサーバ3へ送出する（ステップSP9）。

【0045】

またWWWサーバ3は、デジタル署名書を受けとると、予め受けとっている利用者証明書に記載された公開鍵を用いてデジタル署名を復号化し、当該復号化が正常に行われた場合、正当な利用端末4から電子有価情報の要求がされた

と判断する。

【0046】

かくしてWWWサーバ3は、電子有価情報にかかる利用者端末4に電子有価情報を送出する準備を行い、当該電子有価情報に対して公開鍵で暗号化し、これにより得た暗号化電子有価情報を利用者端末4に送出することができる。

【0047】

ここでネットワークシステム1においては、図12に示すように、利用者端末4が図13に示す書き込み処理手順RT3に従って書き込みを行うと共に、セキュリティサーバ6が図14に示す書き込み処理手順RT4に従って暗号化電子有価情報を復号化してすることにより、利用者端末4が電子有価情報をICカード8に書き込むことができる。

【0048】

まずWWWサーバ3は、暗号化電子有価情報を利用者端末4のWWWブラウザ22に送出する。

【0049】

利用者端末4のCPU10は、WWWブラウザ22において暗号化電子有価情報を受けとると、書き込み処理手順RT3を開始し（ステップSP21）、受けとった暗号化電子有価情報及び復号要求コマンドC3を暗号処理モジュール23に送出する（ステップSP22）。

【0050】

続けてCPU10は、暗号処理モジュール23で受けとった暗号化電子有価情報及び復号要求コマンドC3に合わせて、ICカード読書き装置9を介してICカード8から読み出した使用者IDをセキュリティサーバ6へ送出する（ステップSP23）。

【0051】

セキュリティサーバ6のCPU46は、復号要求コマンドC3を受けとると、書き込み処理手順RT4を開始し（ステップSP41）、まずICカード8の認証を行う。CPU46は、受けとった使用者IDに対応する共通鍵を共通鍵データベース55から読み出し（ステップSP42）、当該読み出した共通鍵で共通

暗号化情報を生成する。続けてCPU46は、共通暗号化情報及びICカード認証要求コマンドC4を利用者端末4の暗号処理モジュール23に送出する（ステップSP43）。

【0052】

利用者端末4のCPU10は、暗号処理モジュール23においてICカード認証要求コマンドC4及び共通暗号化情報を受けとると、ICカードドライバ21を操作（ステップSP24）することによりICカード読書き装置9を介してICカード8にICカード認証要求コマンドC4及び共通暗号化情報を送出する。

【0053】

ICカード8は、ICカード認証要求コマンドC4を受けとると、かかる共通暗号化情報を内部に設けられたEEPROM31内の共通鍵で認証（復号）し、当該認証結果を暗号処理モジュール23を介してセキュリティサーバ6に送出する（ステップSP25）。

【0054】

セキュリティサーバ6のCPU46は、暗号処理モジュール23から送出された認証結果を受けとり（ステップSP44）、当該認証結果によりICカード8の認証が正常に行われたことを確認すると（ステップSP45）、利用者証明データベース55（図6）から利用者IDの秘密鍵を取得し（ステップSP46）、この秘密鍵で暗号化電子有価情報を復号化する（ステップSP47）ことにより、電子有価情報を生成する。

【0055】

続けてCPU46は、生成した電子有価情報を共通鍵データベース55から読み出した共通鍵で暗号化して、共通暗号化電子有価情報を生成する。

【0056】

一方CPU46は、受けとった認証結果によりICカード8の認証が正常に行えなかったことを確認すると（ステップSP45）、利用者端末4から利用者IDを受けとり、当該利用者IDに応じた共通鍵に対してICカード8内で認証を行い、当該認証結果を受けとるようになされている。

【0057】

利用端末4のCPU10は、暗号処理モジュール23において、セキュリティサーバ6から書き込み要求コマンドC5及び共通暗号化電子有価情報を受けとる（ステップSP27）と、当該共通暗号化電子有価情報をICカード読書き装置9を介してICカード8に送出する。

【0058】

ICカード8のCPU27は、受けとった共通暗号化電子有価情報をEEPROM31の共通鍵用エリア34から読み出した共通鍵で復号化し、当該復号化して得た電子有価情報をEEPROM31の電子有価情報用エリア33に書き込む。

【0059】

また利用端末4のCPU10は、暗号処理モジュール23において受けとった電子有価情報をWWWブラウザ22に送出する。かくしてWWWブラウザ22は、WWWサーバ3から復号化された電子有価情報を得ることができる。

【0060】

（3）本実施の形態の動作及び効果

以上の構成において、このネットワークシステム1では、セキュリティサーバ6がWWWサーバ3から与えられる利用者の認証要求に応じて、当該利用者が携帯するICカード8に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行い、当該利用者を認証できた場合にのみ、WWWサーバ3に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行う。

【0061】

従ってこのネットワークシステム1によれば、セキュリティサーバ6がWWWサーバ3から与えられる利用者の認証要求に応じて、共通鍵暗号方式による当該利用者の認証を行い、当該利用者を認証できた場合にのみ、WWWサーバ3に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うことにより、共通鍵暗号方式による高速性と公開鍵暗号方式による安全性とを合わせ持つことができる。

【0062】

以上の構成によれば、このネットワークシステム1において、セキュリティサ

サーバ6がWWWサーバ3から与えられる利用者の認証要求に応じて、共通鍵暗号方式による当該利用者の認証を行い、当該利用者を認証できた場合にのみ、WWWサーバ3に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うことにより、共通鍵暗号方式による高速性と公開鍵暗号方式による安全性とを合わせ持つことができ、かくして認証に対する安全性及び高速性を向上し得るネットワークシステム1を実現することができる。

【0063】

(4) 他の実施の形態

なお上述の実施の形態においては、カード読み書き装置9とICカード8とが無線を介して情報を受渡しする場合について述べたが本発明はこれに限らず、カード読み書き装置9とICカード8とを物理的に接続して情報を受渡しするようにしても良い。

【0064】

また上述の実施の形態においては、セキュリティサーバ6とICカード8との間で認証を行った後、セキュリティサーバ6で復号された電子有価情報をICカード8に格納する際、再度セキュリティサーバ6とICカード8との間で認証を行ってから当該電子有価情報をICカード8に格納する場合について述べたが本発明はこれに限らず、セキュリティサーバ6とICカード8との間で接続が確立されている限り、セキュリティサーバ6とICカード8との間での認証を1回だけに行うようにしても良い。

【0065】

さらに上述の実施の形態においては、利用者端末4からセキュリティサーバ6に対して共通鍵に基づく認証要求が与えられた際に、ICカード8の認証を行う場合について述べたが本発明はこれに限らず、利用者端末4がインターネットと接続した際にセキュリティサーバ6と接続し、予めICカード8の認証を行っておくようにしても良い。

【0066】

さらに上述の実施の形態においては、電子マネーや定期券情報等の電子有価情報を扱う場合について述べたが本発明はこれに限らず、フリーウェア等の無償の

情報を扱うようにしても良い。

【0067】

さらに上述の実施の形態においては、電子有価情報として電子マネーや定期券情報等を扱う場合について述べたが本発明はこれに限らず、電子有価情報として音楽情報や書籍情報等を扱うようにしても良い。

【0068】

さらに上述の実施の形態においては、情報保持媒体としてＩＣカードを用いる場合について述べたが本発明はこれに限らず、演算機能やメモリ機能を有した媒体であれば良い。

【0069】

さらに上述の実施の形態においては、セキュリティサーバ６が共通鍵で生成した暗号化情報をＩＣカード８において復号化して利用者を認証する場合について述べたが本発明はこれに限らず、ＩＣカード８が共通鍵で生成した暗号化情報をセキュリティサーバ６において復号化して利用者を認証するようにしても良い。

【0070】

【発明の効果】

上述のように本発明によれば、利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させ、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行い、利用者を認証できた場合にのみ、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うようにしたことにより、公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた利用者認証を行うことができ、かくして認証に対する安全性及び高速性を向上させ得る認証システム、認証方法、認証装置及びその方法を実現できる。

【図面の簡単な説明】

【図１】

本実施の形態によるネットワークシステムの構成を示す略線図である。

【図２】

利用者端末の構成を示すブロック図である。

【図 3】

ICカードの構成を示すブロック図である。

【図 4】

WWWサーバの構成を示すブロック図である。

【図 5】

セキュリティサーバの構成を示すブロック図である。

【図 6】

認証の様子の説明に供する略線図である。

【図 7】

利用者端末の認証処理手順のフローチャートである。

【図 8】

セキュリティサーバの認証処理手順のフローチャートである。

【図 9】

共通鍵データベースの構成を示す略線図である。

【図 10】

利用者証明データベースの構成を示す略線図である。

【図 11】

証明書の構成を示す略線図である。

【図 12】

書き込みの様子の説明に供する略線図である。

【図 13】

利用者端末の書き込み処理手順のフローチャートである。

【図 14】

セキュリティサーバの書き込み処理手順のフローチャートである。

【符号の説明】

1 ……ネットワークシステム、 3 ……WWWサーバ、 4 ……利用者端末、 6 ……セキュリティサーバ、 8 ……ICカード、 11 ……暗号処理モジュール、 17、 31、 42、 53 ……CPU、 23、 48、 60 ……外部記憶装置、 61 ……利用者データベース、 62 ……共通データベース。

【書類名】図面

【図1】

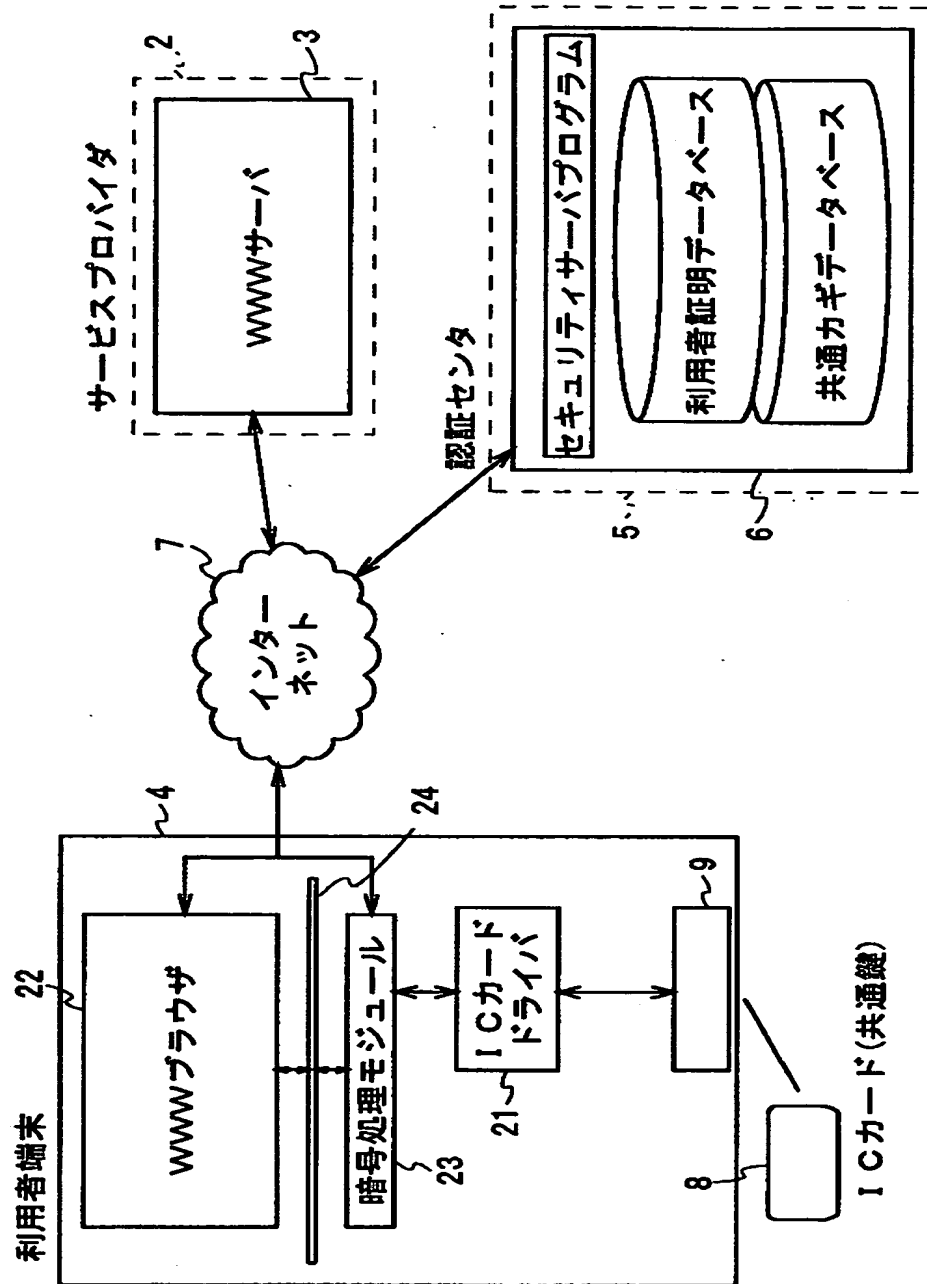


図1 ネットワークシステムの構成

【図2】

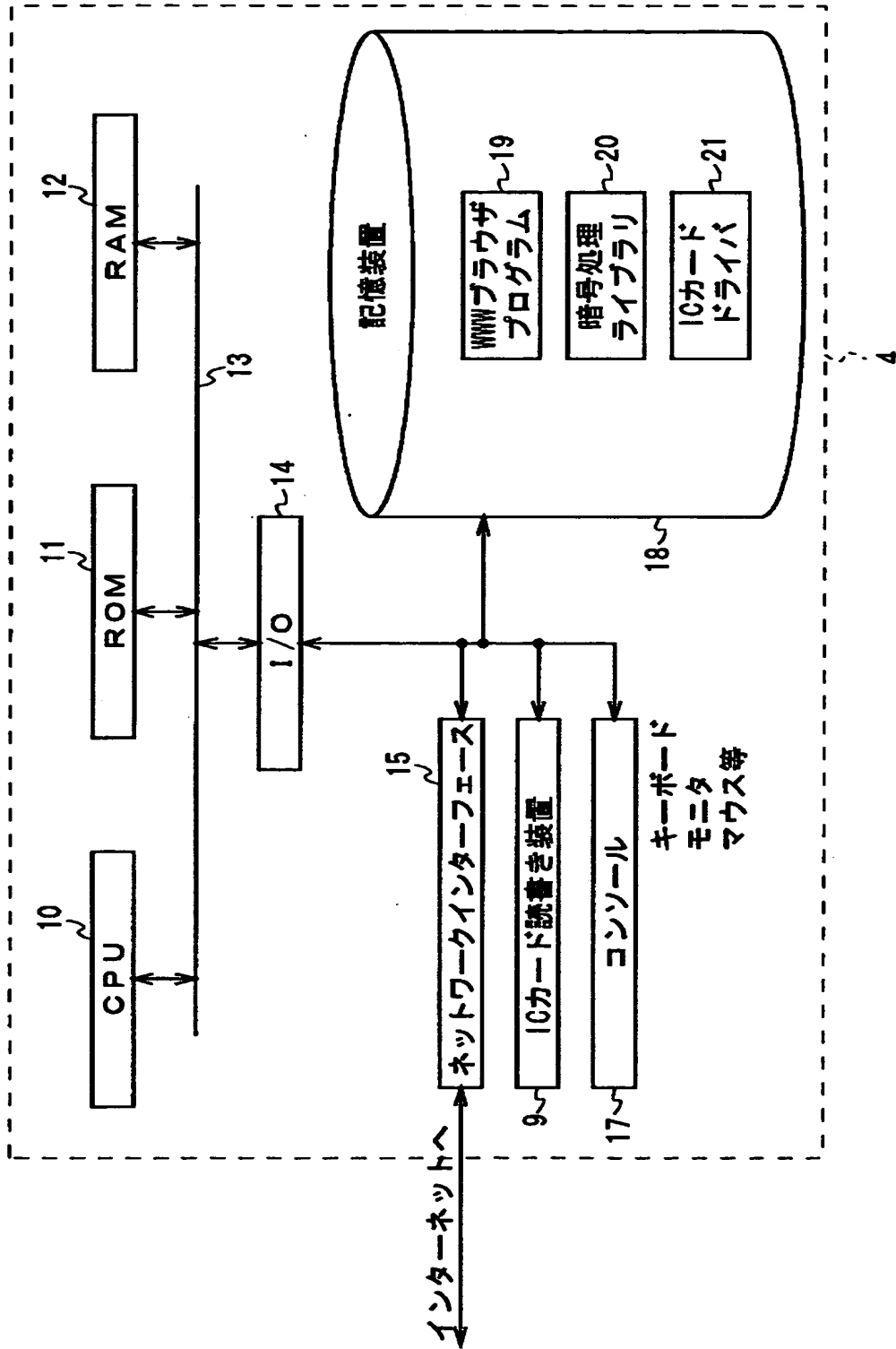
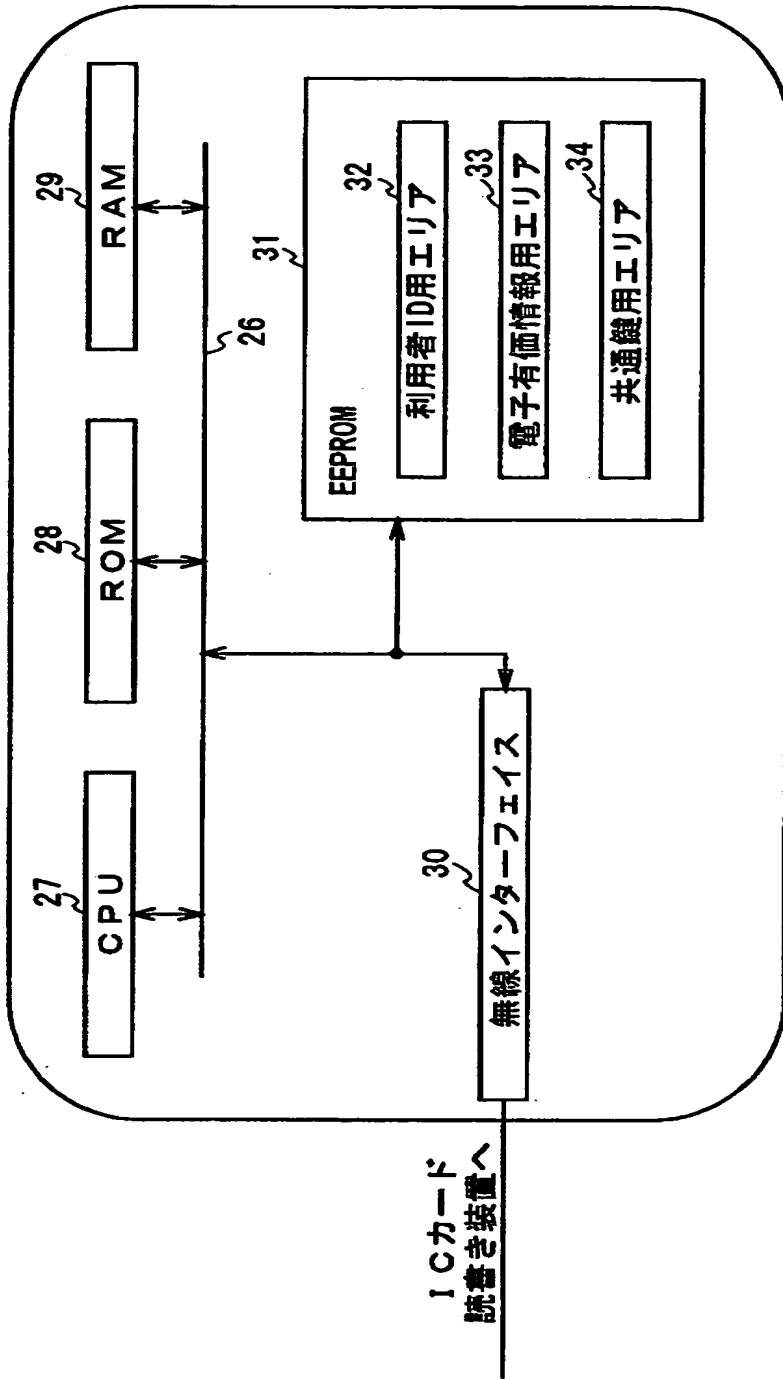


図2 利用者端末の構成

【図3】



8

図3 ICカードの構成

【図4】

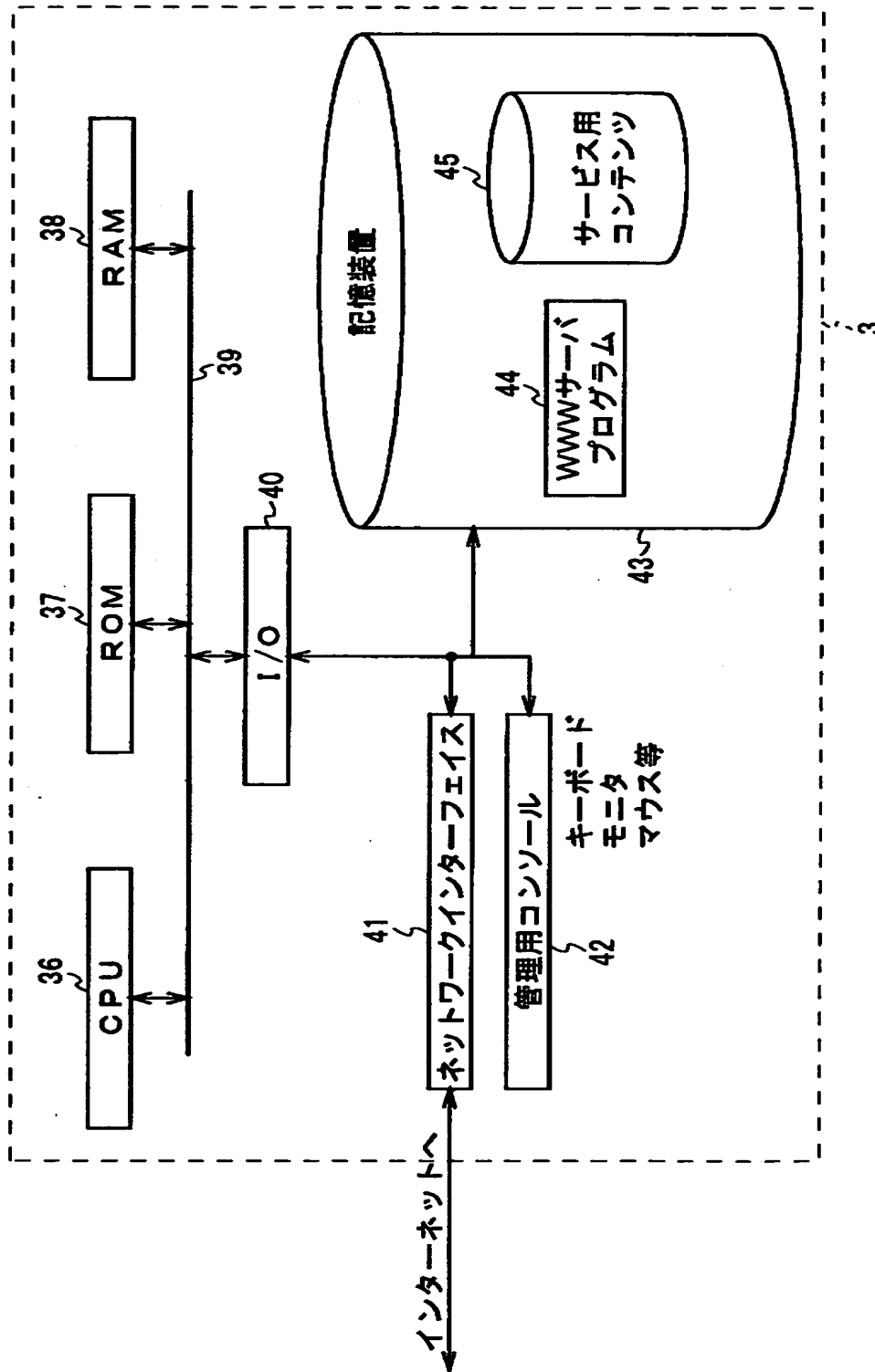


図4 WWWサーバの構成

【図5】

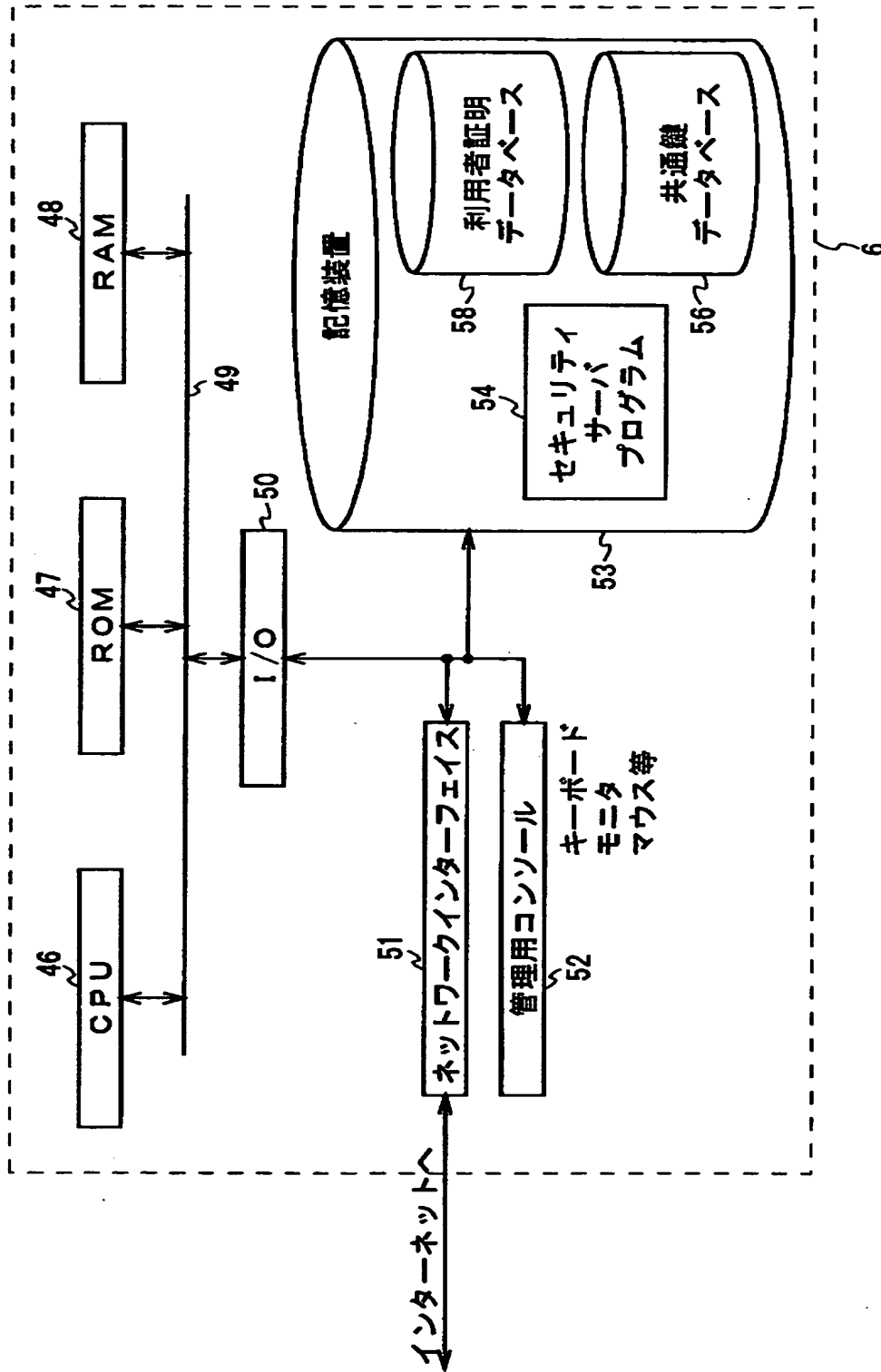


図5 セキュリティサーバの構成

【図6】

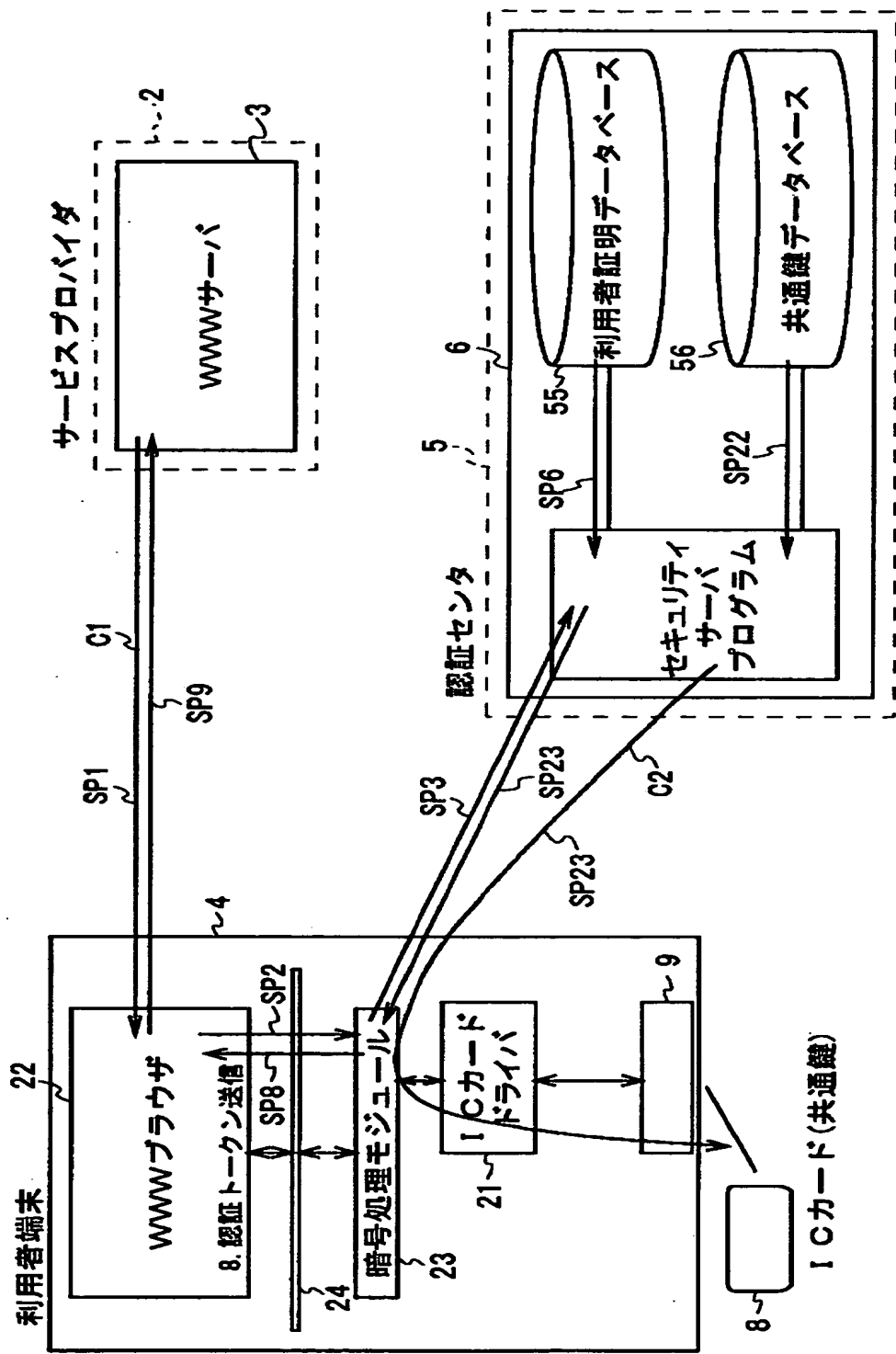


図6 認証の様子

【図 7】

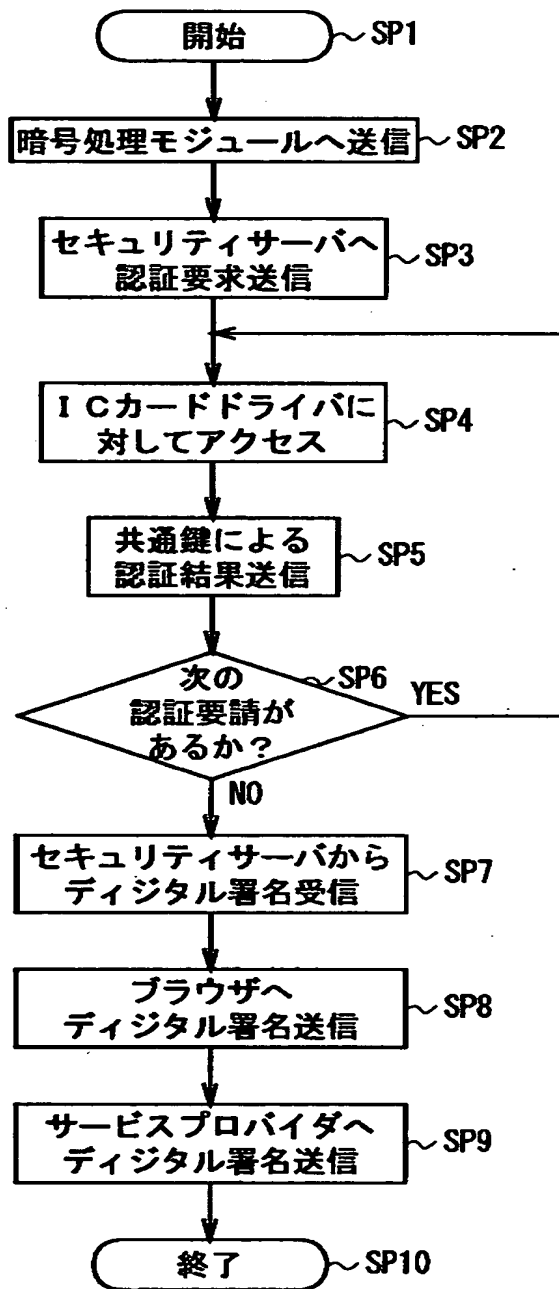


図 7 利用者端末の認証処理手順

【図 8】

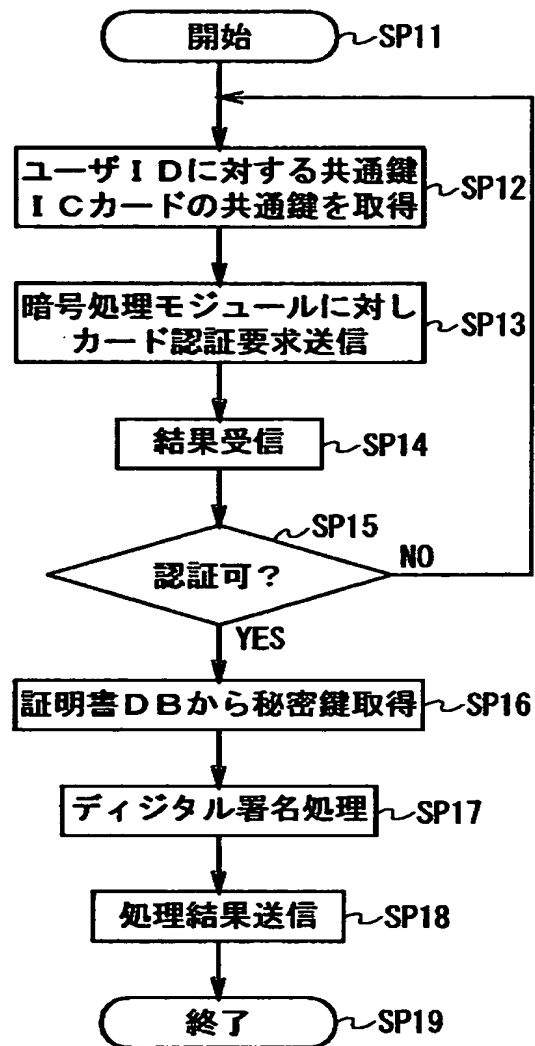


図 8 セキュリティサーバの認証処理手順

【図 9】

利用者 I D	カード用共通鍵
0001	XXXXXXXXXXXXX
0002	XXXXXXXXXXXXX
0003	XXXXXXXXXXXXX
⋮	⋮

56

図 9 共通カギデータベース

【図 1 0】

57 利用者 I D	58 証明書	59 秘密鍵
0001	利用者 I D 0001 の証明書	XXXXXXXXXXXXX
0002	利用者 I D 0002 の証明書	XXXXXXXXXXXXX
0003	利用者 I D 0003 の証明書	XXXXXXXXXXXXX
⋮	⋮	⋮

55

図 1 0 利用者証明データベース

【図 1 1】

証明書シリアルナンバー : 123456789
有効期限 : 2001/12/31
利用者ID : 0001
公開鍵 : xxxxxxxxxxxxxxxx
E-mail : <u>taro@somedomain.com</u>
連絡先 : <u>〇〇県 × × 市 J P</u>

CAの署名

60

58

図 1 1 証明書

【図12】

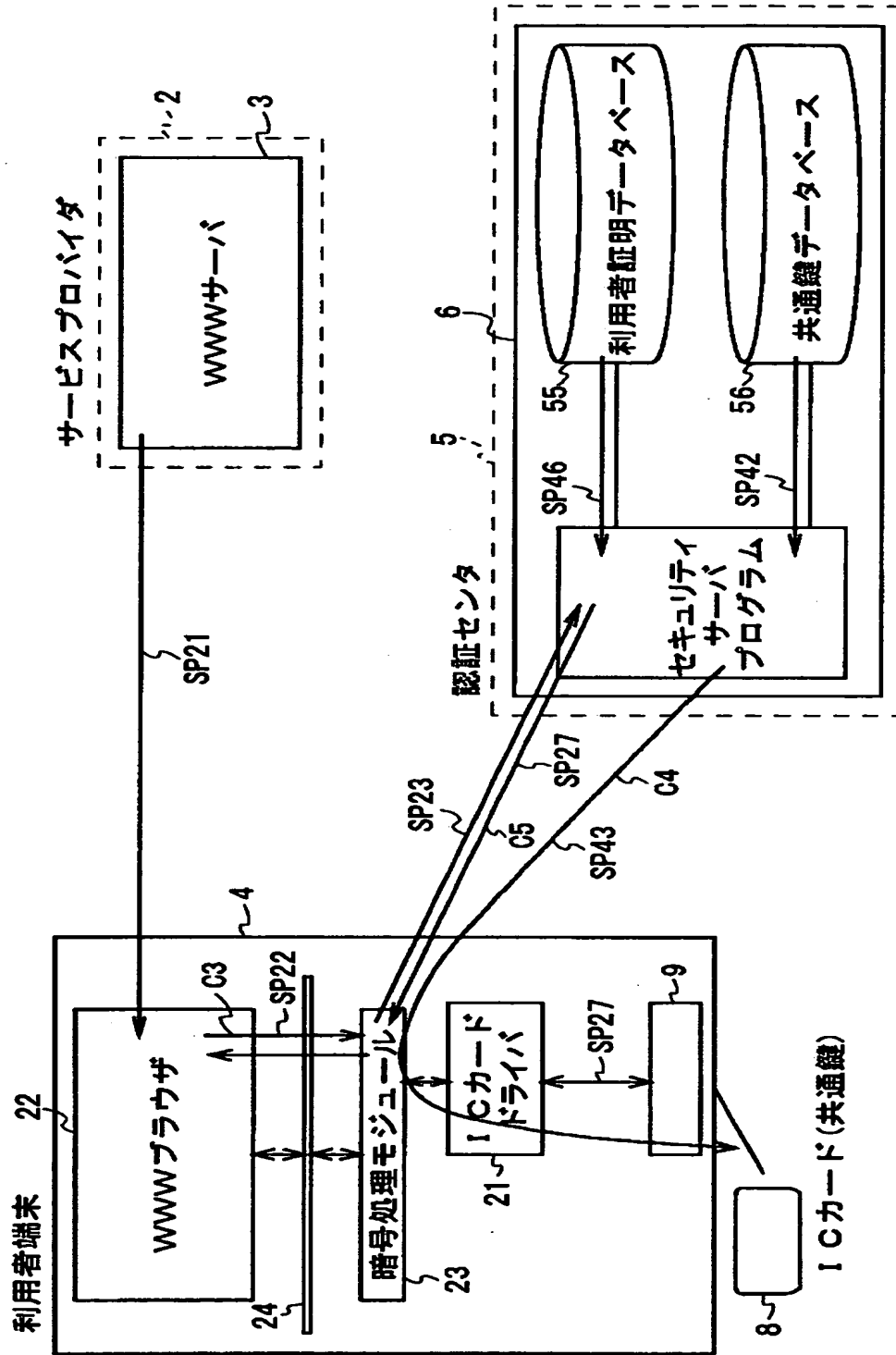


図12 書き込みの様子

【図 1 3】

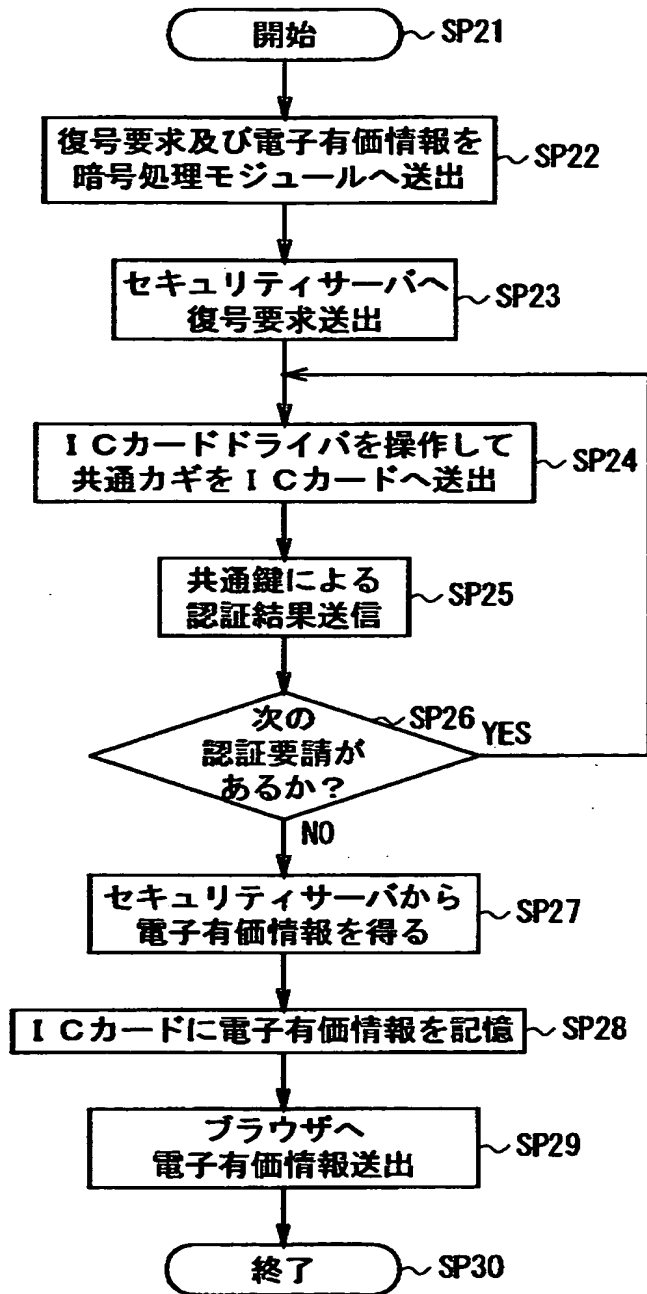


図 1 3 利用者端末の書き込み処理手順

【図 1 4】

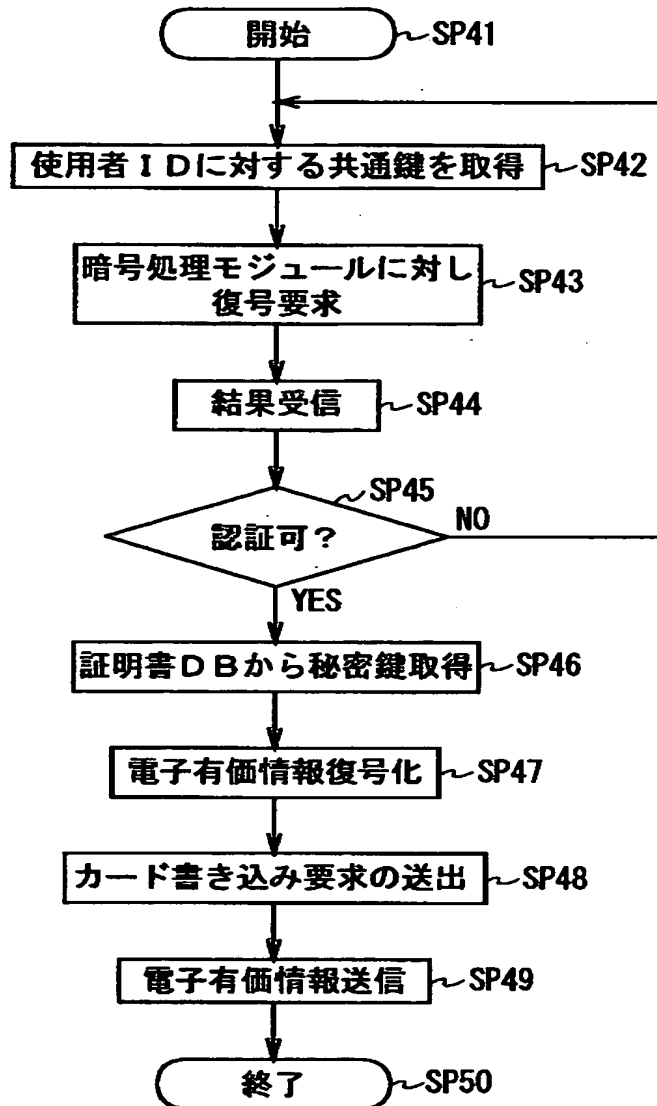


図 1 4 セキュリティサーバの書き込み処理手順

【書類名】 要約書

【要約】

【課題】

公開鍵暗号方式のもつ安全性と共通鍵暗号方式のもつ高速性とを合わせもたせた認証方式が望まれていた。

【解決手段】

利用者の共通鍵暗号方式による共通鍵を情報保持媒体に保持させ、情報処理装置から与えられる利用者の認証要求に応じて、当該利用者の情報保持媒体に保持された共通鍵に基づいて共通鍵暗号方式による当該利用者の認証を行い、利用者を認証できた場合にのみ、情報処理装置に当該利用者の認証を公開鍵暗号方式で行わせるための所定の処理を行うようにした。

【選択図】 図 6

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社